Remarks:

Status of the Claims

In the office action of April 7, 2009 Claims 1, 2, 4-6, 8 and 9 stand rejected.

Claims 1, 5, 6 and 8 are amended herein. Claims 1-2 and 4-6, 8 and 9 are now pending in the application.

The Claims

Claim Objections

Claim 3 was objected for using the word “move” when, in the Examiner’s opinion, the word “moving” would be more appropriate and for not using subscripts for h_1 and h_2, respectively. However, Claim 3 is not pending in the application. It appears that the offending language was used in Claim 5 and with respect thereto, Applicants agree, and have amended the claim as suggested by the Examiner. Applicants posit that all objections to claims are now moot and respectfully request withdrawal of the objections.

35 USC 112, Second Paragraph

Claims 1, 2, 4-6, 8 and 10 were rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner pointed to the use of “if” in defining a *super-function*. Applicants have amended Claim 1, 6, and 8 to more clearly recite the subject matter of the invention, notably rewording the claims to avoid the use of conditional statements. Applicants posit that the claims now meet the requirements of 35 USC 112, second paragraph, and, accordingly, request withdrawal of the rejection.

35 USC 103

Claims 1,2, 4-6, 8 and 9 stand rejected under 35 USC 103(a) as being unpatentable over Lim (U.S. Pat. Pub. 2002/0003876 A1) in view of Kocher (U.S. Pat. No. 6,539,092 B1) as evidenced by Hein, James L. "Discrete Mathematics." Applicants traverse the rejection.

The Supreme Court recently confirmed the long standing principle that an obviousness analysis begins with factual inquiries to (A) determine the scope and content of the prior art, (B) ascertaining the differences between the claimed invention and the prior art, and (C) resolving the level of ordinary skill in the pertinent art. *KSR v. Teleflex,* 82 USPQ2d 1385, 1391 (2007), (*citing with approval, Graham v. John Deere,* 383 US 1, 148 USPQ 459, (1969)).

Furthermore, "there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR,* at 1396, *quoting* (*in re Kahn*, 441 F.3d 977, 988, 78 USQP2d 1329, (Fed. Cir. 2006).

Turning now to the first of these factual inquiries, namely, the scope and content of the prior art. Lim's Figure 1 shows the cipher function of the typical DES algorithm. Lim, [0006]. Figure 1 illustrates the components of the cipher function including the left register L(i-1) and the right register R(i-1). These registers are used in each round of the DES algorithm to produce the input to the subsequent round. For one round, the right register goes through the cipher function. The cipher function consists of an expansion unite 110, an XOR operation 120 in which the output of the expansion unit is XORed with the key, a substitution box (S-BOX) 130, and a permutation box (P-BOX) 140. The output from the P-BOX is XORed with the contents of the left register. What is being disclosed in Figure 1 of Lim is quite simply just the standard DES algorithm cipher function.

Kocher teaches a cryptographic key management mechanism. Kocher's mechanism starts with a seed key K0 and through a defined sequence of operations that depends on a depth parameter can determine a defined sequence of keys. Kocher uses four state update functions FA, FB, FA-1, and FB-1 to produce a sequence of states. Kocher, Col. 4, Lines 35-37. FA-1 is the inverse operation of FA, and FB-1 is the inverse operation of FB. Figure 1 illustrates the sequence. Going from a beginning state with a count variable C=0 and the starting state=K0 (i.e., the initial key) 100 a sequence of secret state values are produced. A counter C determines which key to use and a parameter, index depth D, determines the cycle length of the key update process. Col. 3, Lines 50 – 60.

Consider Figure 1. Each dot in the diagram (e.g., 110, 111) represents a step for performing a transaction using a given key. The dot-to-dot transitions represent computation of a new state given the current value of the count C, the depth, and the previous state (KC). A particular algorithm is used to determine with state update function to use. Figure 2 illustrates the function selection algorithm. Note that in Figure 2, V has been assigned C, and N has been assigned D. Step 220. Thus, the selection box 230 compares the current count (held in V) against the value 2^N-3 (where N is the depth). If that is the case, the FA-1 function is executed to determine the new value for KC, step 235. Other values of C trigger other selection criteria 240, 250, 260 thus predictably computing the correct KC in the sequence.

In summary, Kocher provides for a mechanism to compute a new key from a previous key in a predictable manner so that a client and server both knowing the seed key, the other parameters, and the count, may compute the same sequence of keys.

Turning now to comparing the prior art and the claimed invention. Let's start with a summary of the invention. Applicants provide a solution that is not vulnerable to certain types of attack through the introduction of errors - attacks known as Differential Fault Analysis or Extended Fault Analysis – which attempt to obtain information about one or more data items or operations involved in an algorithm calculation by studying the calculation procedure of the electronic assembly when one or more errors are introduced. Specification, Page 1, Lines 7 – 13. The mechanism used is that a calculation that uses a function f is modified to use a function f' which is referred to as a *super-function.* A *super-function* is defined by the relationship:

$h_2(f'(h_1(x))) = f(x)$

where x is an element of a set E, h1 is defined such that it provides a one-to-one mapping of E into a set E', h2 is defined such that it provides an onto mapping of

F' in F, and for any element x in E, the above equality holds. As a result, in lieu of performing the operation f(x), the super-function f' may be performed together with ancillary mappings.

Furthermore, because a Differential Fault Analysis attack uses the introduction of errors, it is useful to perform error detection on intermediate results.

Accordingly, Applicants claim executing a super-function and performing a validation check:

"performing the calculation of f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f'" and "performing the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature" (Claim 1).

For the first of these limitations the Examiner points to Lim's description of the CIPHER unit for a DES algorithm. The Examiner asserts that Lim teaches performing an elementary operation using a super-function at Fig. 1, elt 130 (because this operation has a 48-bit input and a 32-bit output) of a function f for which the Examiner relies on Fig. 1, elt CIPHER FUNCTION. Office Action, Page 4, Lines 8 – 13. This is an incorrect reading of Lim.

If we consider Lim's CIPHER FUNCTION as f(x), then all the Lim has described is how to implement f(x) in terms of sub operations peformed by particular units. Lim has not taught or suggested performing the caluclation of f(x) by performing the elementary operation f(x) using a super-function (Claim 1).

A super-function is precisely defined in the claim to be a function that satifies the equality "$h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F, wherein x is a member of E and f(x) is a member of the set F." The *super-function* is a substitution function that together with the other mapping operations provide the same result as the function. Lim does not disclose one set of functions to be a substitute for another function. Rather Lim explains how the CIPHER function is to be performed using the expansion permutation 110, the S-BOX 130, and the P-Box 140. However, Lim does not teach or suggest that any of these operations can be performed using a *super-function* of any one of the operations.

For the foregoing reasons, Claim 1 is patentable over Lim.

The Examiner turns to Kocher for teaching of the verification function. This is an incorrect reading of Kocher. The Examiner points to two passages of Kocher, namely, Col. 6, Lines 8-24 and Col. 7, Lines 1 – 27. As noted above, Kocher teaches a key management system in which a sequence of keys are predictably computed so as to allow for a client and server to both know the same key for a transaction in a sequence of transactions. Col. 6, Lines 8-24 is part of the description of Figure 2. Figure 2 is a flow-diagram illustrating the process of incrementing the sequence counter C and deciding which of four functions to apply to calculate the next sequence state. Kocher, Col. 5, Lines 64 – 67. The first cited passage describes steps 230 through 265. For each of the selection criteria of steps 230, 240, 250, and 260, the counter C is incremented and a particular function is used to calculate the new key, e.g, in step 235 the function FA-1 is used to calculate the key. There is no discussion in this passage that relates to computing a verification function. Further, in each instance the calculation is to compute the next key in a sequence of keys from the previous key. That cannot be considered "using the result obtained by the super function."

The second cited passage corresponds to a Figure 3. Figure 3 is the server-side process that corresponds to the client-side process of Figure 2. Kocher, Col. 6, Lines 54 – 55. Similarly to the client-side process, the appropriate function for computing the key is determined. Again, there is no discussion of verification of an intermediate result.

In making the argument based on Kocher, the Examiner states that "Kocher teaches performing an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature." Office Action, page 5, Lines 3-6. Is the examiner asserting that the key KC of Kocher is the intermediate result and that the calculation of the next key in the sequence is the calculation signature? If so, Applicants could not disagree more. A key is not a calculation signature of an intermediate result.

Claims 6 and 8 recite analogous limitations to the limitations argued in support of Claim 1. These claims are patentable over the combination of Lim and Kocher for, at least, the reasons given in support of Claim 1.

Claims 2, 4, 5, and 9 depend from Claim 1, inherit the limitations thereof, provide further unique and non-obvious combinations, and are patentable for the reasons given in support of Claim 1 and by virtue of such further combinations.

For the foregoing reasons, the combination of Lim and Kocher taken singly or in combination does not result in Applicants' claimed invention.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: August 20, 2009

/Pehr Jansson/
Pehr Jansson

Registration No. 35,759

The Jansson Firm
3616 Far West Blvd #117-314
Austin, TX 78731
512-372-8440
512-597-0639 (Fax)
pehr@thejanssonfirm.com